CYWARE™

Cyware Situational Awareness Platform (CSAP)

A real-time threat information sharing and communication platform for faster and better informed cyber threat response

More and more, security teams are putting their businesses at ever-greater risk by failing to keep up with the increasing volume of alerts and to comprehend these risks given the constantly changing threat environment truly. Compounding the problem is the singular nature of most security tool interfaces (too many screens) and the lack of cross-communication within security teams.

Security teams need a solution that enables them to efficiently deal with security alerts and do so more effectively through better communication, greater collaboration, and expanded knowledge of the threat landscape to get ahead of the situation. They need a tool that will allow them to more quickly collect, analyze, and respond to alerts in real-time, thus reducing the organization's overall cyber risk exposure.

Cyware Situational Awareness Platform (CSAP) is a real-time threat information sharing and communication platform that enables you to share accurate and actionable strategic threat intelligence systematically. CSAP automatically aggregates threat alerts and equips security teams with information to improve situational awareness and resilience. CSAP's unique mobile capability is the underpinning for a powerful "On-the-Go" availability of information and platform access that empowers security teams to take action in real-time or warn security teams of an immediate crisis.

CSAP is truly a cybersecurity force multiplier. Its strategic threat intelligence-driven approach ensures faster and better-informed responses. It drives collaboration between security teams, breaks down communication silos and improves overall security team efficiency and effectiveness.

CSAP Capabilities

Strategic Threat Intelligence Sharing

- Automated intel ingestion & dissemination
- On-the-go sharing via mobile
- Analyst enrichment and anonymization
- Mitre ATT&CK™ Heat Mapping
- Directed sharing based on role, location and/or business group

Complete Threat Communication

- Custom alerts and notifications
- Automated RSS conversion and alerting
- Out-of-band crisis notification
- Mobile-enabled communication via sms, CSAP mobile app, voice call or email

Advanced Alert Orchestration

- Multi-source ingestion, aggregation, and noise removal Analyst interaction
- Remote alert actioning via mobile
- Automated email ingestion and conversion

Enhanced Security Collaboration

- Trusted sharing communities
- Encryption-based secure messenger
- Mobile-enabled incident reporting
- One-click security support
- Customizable metrics-based reporting

CSAP Benefits: Understand, Action and Collaborate

Gain a Better Understanding of The Threat Landscape

- Deploy a strategic threat intel-driven approach to exchange and manage alerts on incidents, breaches, and security trends to ensure end-users are aware of the cyber threats facing your security team.
- Automate alerts from various sources into human-readable security updates and receive real-time information on new threats, techniques, and malware without having to look at multiple sources manually.
- Gain greater visibility of existing and emerging threats through actionable, information sharing.

Improve Cyber Awareness & Resilience

- Create, receive, and share real-time role, location, and business purpose-based alerts via the web, email, or mobile to power constant, reliable situational awareness.
- Aggregate unique OSINT threat intelligence feeds and vulnerability & malware early notifications to provide actionable alerts with employees, vendors, customers, peers, information sharing communities, and more.
- A new sleek messenger to boost communication, engagement, and information sharing between various internal teams and key stakeholders, such as CISO, SOC Manager, Analysts, etc., through threat-specific discussions in a closed and trusted environment.

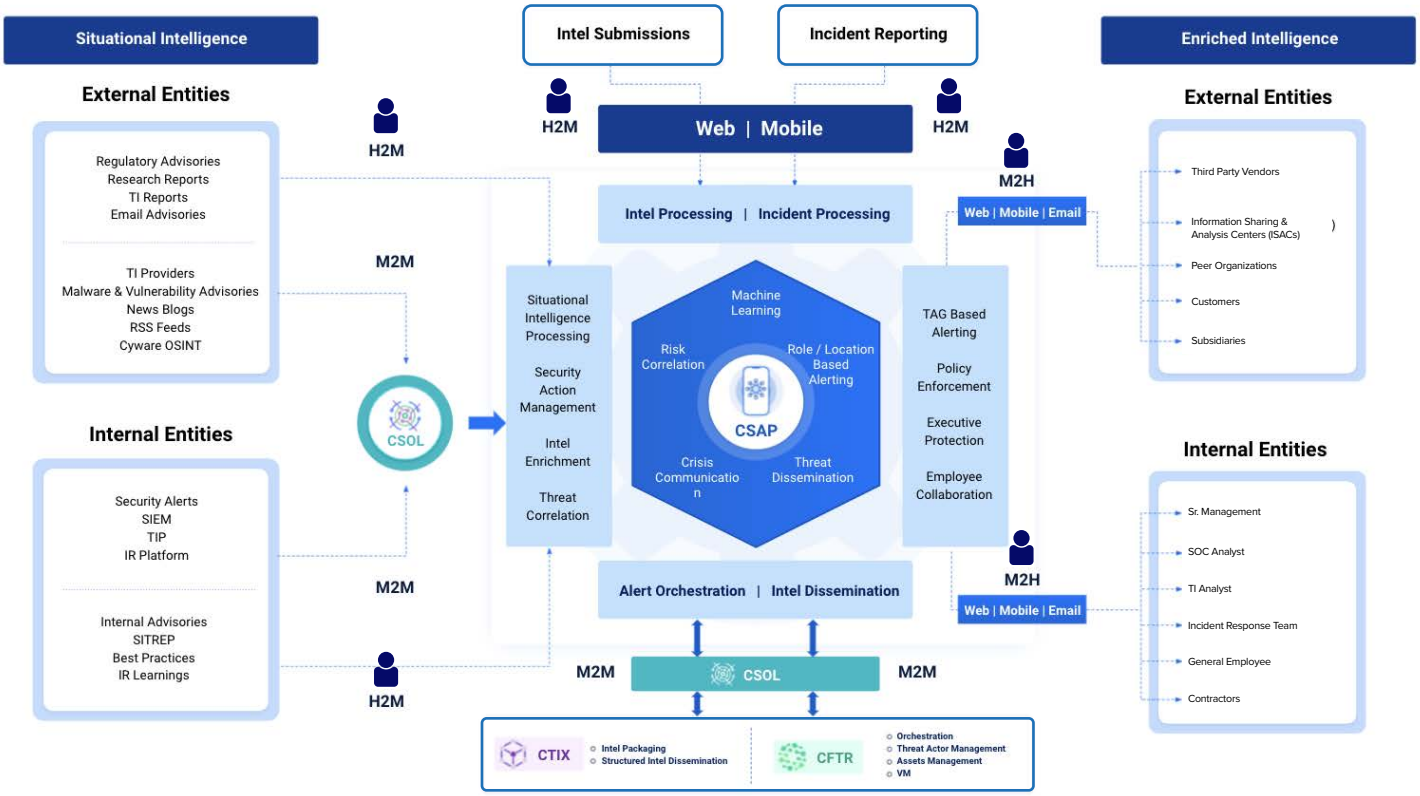
Faster and More Informed Responses = Better Decisions

- Deliver alerts automatically from SIEM tools, threat intelligence platforms; Intel feeds and vulnerability scanning tools, etc., to those who need to take action.
- Equip SecOps teams with automated threat intelligence ingestion and dissemination capabilities to quickly identify, prioritize, and respond to threats.
- Orchestrate all security alerts into both human and machine-readable formats for AI-enhanced and prioritized alerts ready for human decision-making.

Mobile-enabled Communication & Actioning Anytime, Anywhere

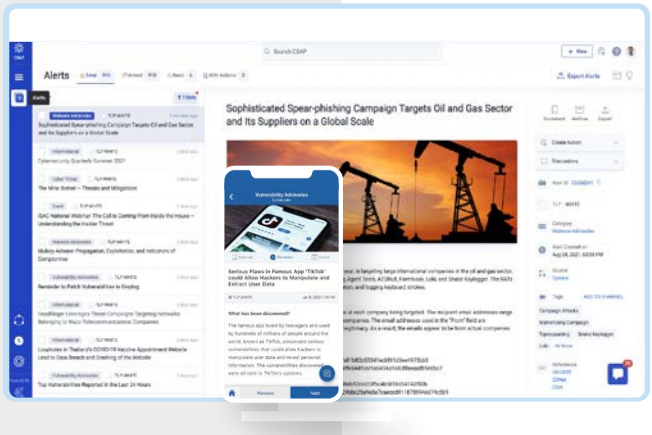
- Strengthen your first line of defense through actionable, real-time cyber situational awareness and incident response within a single, streamlined platform.
- Share accurate and actionable strategic threat intelligence over mobile and web apps, with or without analyst intervention, for faster threat detection, analysis, and response.
- Rapidly alert all or a select group of employees in case of emergencies, like a large malware outbreak or major vulnerability disclosure, using the Crisis Notification feature.

CSAP Architecture



Collaborative Cyber Threat Defense Made Easy

- Share real-time security alerts and crisis notifications with your security teams and employees
- Empower security teams and employees to share strategic threat intelligence through mobile
- Better organization of files inside the Doc Library for accessing the files quickly and with ease
- Aggregate threat alerts from all internally deployed tools
- Ability to do personalized branding of the entire platform for all CSAP administrators
- Guided Walkthrough and Tutorial Videos to promote self-learning among users
- Users can now avoid clutter by customizing the Alert feed layout within the CSAP Member Portal



The CSAP Advantage

CENTRALIZED DASHBOARD
Manage all security alerts using a single, centralized, easy-to-use dashboard with performance metrics, graphs providing insights into alerting, intel sharing, and user activity.

CYWARE ALERTS
Gain access to unlimited real-time, expertly analyzed, and enriched threat alerts to proactively neutralize risks from malware, vulnerabilities, and data breaches to stay ahead of the bad actors.

THREAT INTEL ACTIONS
Initiate and assign follow up actions to security analysts based on the received strategic threat intelligence

DETAILED REPORTS AND METRICS
Create and view reports based on various metrics and gain in-depth insight into your organization's security readiness.

INTEL EXTRACTION
Extract Intel in a standardized format from a URL with just a click of a button on your mobile device and quickly share it with security teams.

IOC SHARING
Develop a potent defensive mechanism against threats by proactively sharing IOCs through your mobile device.

COLLABORATION
Enable security teams to join forces in real-time and curate thoroughly enriched threat intelligence

SURVEY TOOL
Garner the opinion of your security teams and employees on various issues, measure if your message is being heard, and create more impactful company policies through targeted surveys.

SPEEDBUMP
Prevent inadvertent and accidental sharing of information by analysts using the Speedbump feature in threat alert publishing workflow.

MESSENGER
Collaborate with cross-functional teams over the built-in Secure Messenger

Deployment Environments

We provide multiple deployment options for our products, giving our customers the flexibility to make use of all the product features by choosing the best model that suits their business needs.

Public and Private Cloud

On-Premise

System Requirements

System requirements will change based on the considerations of high availability and backups.

Operating System

16 CPU Cores

32 GB Memory

100 GB Storage

About Cyware

Cyware helps enterprise cybersecurity teams build platform-agnostic virtual cyber fusion centers. Cyware is transforming security operations by delivering the cybersecurity industry's only Virtual Cyber Fusion Center Platform with next-generation SOAR (security orchestration, automation, and response) technology. As a result, organizations can increase speed and accuracy while reducing costs and analyst burnout. Cyware's Virtual Cyber Fusion solutions make secure collaboration, information sharing, and enhanced threat visibility a reality for enterprises, sharing communities (ISAC/ISAO), MSSPs, and government agencies of all sizes and needs.

Cyware®

228 Park Ave S, #77147, New York New York - 10003-1502

cyware.com | sales@cyware.com | 855-MY-CYWARE